# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/397,503 | 09/17/1999 | GAURAV AGGARWAL | YO999-129 | 8826 |

7590 07/30/2003

McGINN & GIBB PPLC
8321 OLD COURTHOUSE RD., STE. 200
VIENNA,, VA 22182

| EXAMINER | |
|---|---|
| ZIA, MOSSADEQ | |
| **ART UNIT** | **PAPER NUMBER** |
| 2134 | 9 |

DATE MAILED: 07/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.



3

| Office Action Summary | Application No. | Applicant(s) |
|---|---|---|
| | 09/397,503 | AGGARWAL ET AL. |
| | **Examiner** | **Art Unit** |
| | Mossadeq Zia | 2134 |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 July 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 November 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *1* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

## DETAILED ACTION

### *Specification*

1. The disclosure is objected to because of the following informalities:

- In regards to cross-reference to related patent application (page 1 & 52), the application numbers are missing.
- On page 32, line 6; reference to label 311 is missing from drawing. On same page, line 8, label 312 is not a reader, but a processor in Figure 3. Related errors continue to surface on pages that follow, such as comparator 413 is not a comparator in drawing.

Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 20 and 30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- In regards to claim 20 there is insufficient antecedent basis for a sequence of data and certificates associated with the sample.
- In regards to claim 30, there is insufficient antecedent basis for new data and a certificate associated with the sample.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 2, 3, 4, 7, 14, 20,21, and 23-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Patent No. 5,434,917 Naccache et al.

- In regards to claims 1, 35, and 36, Naccache discloses a method of guaranteeing authenticity of an object (see fig. 2:14) comprising: providing a random sample (see col. 1, lines 34-42), associating a reproducible number that is obtained by a reader reading sample (see fig. 2:23) then forming a coded version of number, and recording the number into the object (see abstract and col. 1, lines 47-55).
- In regards to claim 2, Naccache discloses the use of objects including smart card with method where the number associating to sample, which is essentially reproducible, is recorded onto object. Naccache further discloses the usage of a chip with recording support on the object (abstract and fig. 2:13).
- In regards to claim 3, Naccache discloses the object as a smart card (see col. 1, line 29-32).
- In regards to claim 4, Naccache discloses the usage of a chip with smart card (see abstract and fig. 2:13).
- In regards to claim 7, Naccache discloses the use of public key cryptography where it is part of a digital signature scheme (see col. 1, lines 52-56).

- In regards to claim 14, Naccache discloses sensing a degeneration of sample (see col. 1, lines 35-37 and col. 3, lines 40-47) whereby the object has markings that are detected by the reader and trigger scanning of sample, which implies that reader would sense the condition of marking and respond accordingly if sample were degenerated.
- In regards to claim 20, Naccache discloses that the data associated with a sample is precomputed by an issuing authority (see col. 1, lines 47-48).
- In regards to claims 21 and 30, Naccache discloses that the data associated with a sample is computed dynamically (see col. 1, lines 47-54).
- In regards to claim 23, Naccache discloses a reader (fig. 2:22) reading information from sample (see fig. 2:14) by scanning entire object.
- In regards to claim 24, Naccache discloses sample includes usage of mineral (see fig. 1:11), any other material, and element for randomness whereby sample is affixed to object (see col. 3, lines 40-44).
- In regards to claim 25, Naccache discloses a coded version of number includes one of optional data appended to it (see col. 3, lines 1-10).
- In regards to claim 26, Naccache discloses data linked to sample is selectively changeable (see col. 1, lines 47-54).
- In regards to claim 27, Naccache discloses sample is changeable over time (see col. 1, lines 47-54).
- In regards to claims 28-29, Naccache discloses data is selectively changeable when sample is changed (see col. 1, lines 47-54).

- In regards to claim 31, Naccache discloses coded version of sample that is stored in memory of object is used for comparison when object is presented for authentication (see col. 2, lines 17-36).
- In regards to claim 32, Naccache discloses plurality of coded version numbers are recorded into object (see col. 1, line 53).
- In regards to claims 33 and 34, Naccache discloses a method that prevents imitating, or cloning (see col. 1, lines 28-29) of object comprising: providing a random sample, associating a number that is obtained by a reader, forming a coded version of number, and recording the number onto the object (see abstract and col. 1, lines 47-55).

### *Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 5, 6, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,434,917 Naccache et al. in view of Patent No. 5,499,294, Friedman.

- In regards to claim 5, Naccache discloses everything as claimed above (see claim 1) but fails to clearly disclose that key signature is done with a separate processor.

Friedman discloses that an encryption processor is embedded inside a reader (see fig. 3a:10, 12). The reader (see fig. 3a:11, col. 3, lines 62-63) reads samples and sends data to a the processor (see fig. 3a:12) containing a secure hash function known by the public (col. 5, lines 56-63, col. 6, lines 34-37) and a secret key comprising a public key signature (see fig. 3b). Friedman teaches that the advantageous characteristic of hash is that changing a single bit in the original message input would produce different hash output if subjected to the same hash function (see col. 3, lines 34-38). In order to create a digital signature, the original message is retained unaltered and only the hash is altered by encryption with a private key. Message is authenticated by decrypting the message's unique digital signature using the public key (see col. 3, lines 46-57) where the hash from the digital signature is compared with the recreated hash from the original unaltered message. Therefore, it would have been obvious to one having ordinary skill in the arts at the time of the invention that one would be motivated to modify Naccache as per teaching of Friedman in order to gain the advantage of producing digital signature so that integrity and the authenticity of data can be later tested (see col. 3, lines 47-55).

- In regards to claim 6, Naccache and Friedman disclose everything claimed as applied above (see claim 5), in addition Naccache teaches that a second reader (see fig. 2:24) to extract number and coded version from object (see abstract and col. 3, lines 15-30). The object is deemed authentic when the information from the

coded version using public key signature scheme and number are compatible (see col. 1, line 59-63).

- In regards to claim 22, Naccache discloses everything as claimed above (see claim 1) but fails to clearly disclose private key cryptography as part of the key signature scheme.

  Friedman teaches that the advantageous characteristic of hash is that changing a single bit in the original message input would produce different hash output if subjected to the same hash function (see col. 3, lines 34-38). In order to create a digital signature, the original message is retained unaltered and only the hash is altered by encryption with a private key. Message is authenticated by decrypting the message's unique digital signature using the public key (see col. 3, lines 46-57) where the hash from the digital signature is compared with the recreated hash from the original unaltered message. Therefore, it would have been obvious to one having ordinary skill in the arts at the time of the invention that one would be motivated to modify Naccache as per teaching of Friedman in order to gain the advantage of producing digital signature so that integrity and the authenticity of data can be later tested (see col. 3, lines 47-55).

7. Claims 8, 12, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,434,917, Naccache et al. in view of Patent No. 5,974,150, Kaish.

- In regards to claim 8, Naccache discloses everything as claimed above (see claim 1), however fails to show that the reading is done in an imprecise manner such that sequential readings are not exactly the same.

Kaish discloses a method with readers that reads from a sample where sampling done in an imprecise manner such that sequential readings are not exactly the same. Kaish teaches sampled authentication process as statistical in nature and that a threshold may be applied to define acceptable error rate (see col. 12, lines 47-49) during a authentication process. Kaish further teaches that a random sample has elements that are distinct, detectable, and disposed in an irregular pattern (see abstract), which results in variation in sampling of the same object thus making it imprecise by nature. For readings to be relatively reliable, wherein deformation of data or patterns exist. Such imprecise readings of samples may be "resolved through mathematical analysis using known techniques" (see col. 12, lines 36-39) such as fault tolerant encoding schemes wherein statistical correlation between first reading (see col. 18, lines 30-33) and second reading distinguishes object as authentic from counterfeit (see col. 18, lines 28-34). Therefore, it would have been obvious to one having ordinary skill in the arts at the time of the invention that one would be motivated to further modify Naccache as per teaching of Kaish to gain the advantage of determining a threshold to improve authentication of object by allowing multiple reading of a sample wherein statistical correlation that distinguishes authentic from counterfeit with a specific degree of certainty (see col. 18, lines 28-35).

- In regards to claim 12, Naccache and Kaish disclose everything as applied above (see claim 8), in addition Kaish teaches a comparing step that show that the read

samples, N(R(S)) and N(RO(SO )), are compared against a threshold (see Kaish col 12, lines 45-50 and col 18, lines 28-34).

- In regards to claim 19, Naccache discloses everything as claimed above (see claim 1) however fails to disclose that the object comprises of a piece of paper.

  Kaish discloses an authenticating method where dichroic fibers can be mixed into pulp to form paper (see col. 15, lines 1-5) that results in randomly distributed non-reproducible sample. This can be printed into certificates that are self-authenticating (see col. 16, lines 27-39). Therefore, it would have been obvious to one having ordinary skill in the arts at the time of the invention that one would be motivated to further modify Naccache as per teaching of Kaish to allow an object to be made of a piece of paper because the randomly distributed fiber will produce unique identifying features to be used for sampling and generating authentication data.

8. Claims 9-11,13, and 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No. 5,434,917, Naccache et al. in view of Patent No. 5,974,150, Kaish in further view of Patent No. 5,499,294, Friedman.

- In regards to claim 9, Naccache and Kaish disclose everything as claimed above (see claim 8) however, both fail to clearly disclose that a key signature is done with a separate processor.

  Friedman discloses that an encryption processor is embedded inside a reader (see fig. 3a:10, 12). The reader (see fig. 3a:11, col. 3, lines 62-63) reads

samples and sends data to a the processor (see fig. 3a: 12) containing a secure hash function known by the public (col. 5, lines 56-63, col. 6, lines 34-37) and a secret key comprising a public key signature (see fig. 3b). Friedman teaches that the advantageous characteristic of hash is that changing a single bit in the original message input would produce different hash output if subjected to the same hash function (see col. 3, lines 34-38). In order to create a digital signature, the original message is retained unaltered and only the hash is altered by encryption with a private key. Authentication of message is done by decrypting the message's unique digital signature using the public key (see col. 3, lines 46-57) where the hash from the digital signature is compared with the recreated hash from the original unaltered message. Therefore, it would have been obvious to one having ordinary skill in the arts at the time of the invention that one would be motivated to modify Naccache and Kaish as per teaching of Friedman in order to gain the advantage of producing digital signature so that integrity of message and the authenticity of the sender or originator of that message can be tested (see col. 3 47-55).

- In regards to claim 10, Naccache and Kaish and Friedman disclose everything as claimed above (see claim 9), in addition, Friedman teaches that the functionality of a comparator is to compare values, where it receives "hash from calculator (read from sample) and the secure hash (stored in smartcard) from the decryptor. If these two hashes match," (see Friedman col. 2, lines 41-44) the comparator "will indicate authenticity" (see Friedman col. 6, line 51).

- In regards to claims 11, Naccache and Kaish and Friedman disclose everything as applied above (see claim 10), in addition Naccache discloses verifying the coded version against a number by using public part of private key signature, and if number and coded version read by from the chip are compatible, the card is accepted as authentic (see col. 2, 34-36).
- In regards to claim 13, Naccache and Kaish discloses everything as applied above (see claim 12), in addition Naccache discloses a reader that can read coded version from a chip (see fig. 2, 24, and col. 1, lines 30-33) and verifying the coded version against a number by using public part of private key signature, such that if number and coded version read by from the chip are compatible, the card is accepted as authentic (see col. 2, 34-36).
- In regards to claim 15, Naccache discloses everything as applied above (see claim 14), however, Naccache fails to show that sensing includes comparing difference between an actual reading and an original reading vector against a threshold; forwarding a result to the reader to a processor which associates with reading of sample a vector K(NO(RO(SO))), and forwarding the vector to a second processor including a hash function and a secret part of a public key signature scheme.

  Kaish discloses a method for authenticating an object where sample reading of a random and non-reproducible material produces original and actual reading (see col. 18, lines 30-33) that provides a "vector mapping of distinctive detectable elements" of sample (see col. 18, lines 35-38). Thus authentication of

an object is achieved through a statistical tolerance (see col. 28, lines 3-5) based on this vector information (see col. 28, lines 12-15). Kaish teaches such authentication process is statistical in nature, that a threshold may be applied to define acceptable error rate (see col. 12, lines 47-49) during processing. Furthermore, it teaches that vectored data allows sufficient degrees of freedom to reliably authenticate an object (see col. 18, line 40-44).

Friedman discloses that an encryption processor is embedded inside a reader (see fig. 3a: 10, 12). The reader (see fig. 3a: 11, col. 3, lines 62-63) reads samples and sends data to a the processor (see fig. 3a: 12) containing a secure hash function known by the public (col. 5, lines 56-63, col. 6, lines 34-37) and a secret key comprising a public key signature (see fig. 3b). Friedman teaches that the advantageous characteristic of hash is that changing a single bit in the original message input would produce different hash output if subjected to the same hash function (see col. 3, lines 34-38). In order to create a digital signature, the original message is retained unaltered and only the hash is altered by encryption with a private key. Message is authenticated by decrypting the message's unique digital signature using the public key (see col. 3, lines 46-57) where the hash from the digital signature is compared with the recreated hash from the original unaltered message. Therefore, it would have been obvious to one having ordinary skill in the arts at the time of the invention that one would be motivated to further modify Naccache as per teaching of Kaish and Friedman to gain advantage from using vector data to greatly improve the reliability of the authentication method

(see Kaish, col. 18, lines 36-44) and producing digital signatures so that integrity and the authenticity of data can be later tested (see Friedman, col. 3, lines 47-55).

- In regards to claim 16, Naccache and Kaish and Friedman discloses everything as applied above (see claim 15), in addition Naccache and Kaish discloses object (see fig. 2:12) include a chip (see fig. 2:13), wherein a second processor computes a coded version of hash function (see Friedman, col. 5, lines 56-63, col. 6, lines 34-37) of the transformed vector (see Kaish, col. 18, lines 35-38) appended with predetermined optional data (see Naccache , col. 3, lines 1-10) to provide a coded number being put on chip (see Naccache, fig. 2:13) whereupon introducing card to a another or "second" reader, a predetermined different reading of sample is performed (see Naccache , fig. 2:24).
- In regards to claim 17, Naccache and Kaish and Friedman discloses everything as applied above (see claim 16), in addition discloses a method where an actual vector reading KN (see Naccache fig. 2:22) and a second reading with original vector reading KNO (see fig. 2:23) and are compared within a predetermined closeness (see Kaish col. 12, lines 45-50).
- In regards to claim 18, Naccache and Kaish and Friedman discloses everything as applied above (see claim 17), in addition Naccache discloses a reader (see fig. 2:24) for chip (see fig. 2:13) that reads the coded version and verifying coded version against the vector data using public part of the public key signature, and accepting the object as authentic if the vector and the coded version read from chip are compatible (Abstract and C2, lines 29-36).

*Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mossadeq Zia whose telephone number is (703)305-8425. The examiner can normally be reached on 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-8360 for regular communications and (703)305-8208 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-308-3900.

mz
July 17, 2003

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134